ON THE MINIMUM WEIGHT CODEWORDS OF SOME BINARY BCH CODES

D. Augot P. Charpin N. Sendrier
INRIA, Domaine de Voluceau, Rocquencourt,
BP 105, 78153 Le Chesnay Cedex, FRANCE

Abstract: We give the true minimum distances of some BCH codes of length 255 and 511, which were not known. We describe the set of the minimum weight codewords of the BCH codes with designed distance $2^{m-2}-1$.

Notation

We consider binary cyclic codes of length $n = 2^m - 1$. A BCH code C is always a narrow-sense BCH code, and is characterized by its defining-set:

$$I(C) = \{s \in [0, n-1] \mid \alpha^s \text{ is a zero of } C\},$$

where α is a primitive n-th root of unity.

We identify a codeword x with its locators $(X_i)_{1 \le i \le w}$ and with its locator polynomial [3 p. 243],

$$\sigma(z) = \prod_{i=1}^{w}(1 - X_i Z) = \sum_{i=0}^{w} \sigma_i Z^i,$$

where w is the Hamming weight of x.

The power sum symmetric functions of x,

$$A_k = \sum_{i=1}^{w} X_i^k,$$

are related to the σ_i by the Newton's identities [3 p. 245]:

$$\begin{cases} r \le w, & I_r \ : \ A_r + \sum_{i=1}^{r-1} A_{r-i}\sigma_i + r\sigma_r = 0, \\ r > w, & I_r \ : \ A_r + \sum_{i=1}^{w} A_{r-i}\sigma_i = 0. \end{cases}$$

Remark that for each codeword $x \in C$, we have:

$$\forall s \in I(C),\ A_s = 0.$$

We will denote by $B(n, \delta)$ the BCH code of length n and designed distance δ.

BCH codes of length $2^m - 1$, $m = 8, 9, 10$

Mac-Williams and Sloane give A table of BCH codes [3 p. 267], in which the true minimum distance of some BCH codes of length 255 is not known. This table is improved by Cohen [2]; however some cases remain unsolved.

We write the Newton's identities for a given BCH code C and a given weight w, and we check the consistency of the resulting polynomial system;

- if we find a contradiction, then C has no codeword of weight w,
- if we are able to find a solution, we have a codeword of weight w.

This method enables us to complete the table of the minimum distance of the BCH codes of length 255, and to extend our knowledge of BCH codes of length 511. For the latter length we obtain minimum weight codewords which are idempotents of the code. We present some proofs; for instance, the BCH code of length 255 and designed distance 59 (resp. 61) has minimum distance 61 (resp. 63).

Minimum weight codewords of $B(2^m - 1, 2^{m-2} - 1)$

$n = 2^m - 1$ and $\delta = 2^{m-2} - 1$. Since the code $B(n, \delta)$ contains the Reed-Muller code $R(2, m)$, its true minimum distance is δ.

Using the Newton's identities, we prove the following theorem:

Theorem 1: The minimum weight codewords of the BCH code of length $2^m - 1$ and designed distance $2^{m-2} - 1$ are those of the punctured RM code of same length and order 2.

Corollary 1: Let $x \in B(n, \delta)$, $\delta = 2^{m-2} - 1$, such that $\omega(x) = 2^{m-2}$. Then x is a codeword of the punctured RM code $R(2, m)$ - i.e. the set of the locators of x is an $m-2$-dimensional affine subspace of $GF(2^m)$.

Corollary 2: $m > 5$. The automorphism group of the BCH code $B(n, \delta)$ is contained in $GL(2, m)$. The code generated by the set of the minimum weight codewords of $B(n, \delta)$ is strictly contained in $B(n, \delta)$.

References

[1] D. Augot, P. Charpin and N. Sendrier. The minimum distance of some binary codes via the Newton's identities. EUROCODE'90, LNCS, to appear.

[2] G. Cohen. On the minimum distance of some BCH codes. IEEE Transaction on Information Theory, vol. 26, 1980.

[3] F.J. Macwilliams and N.J.A. Sloane. The Theory of Error Correcting Codes. North-Holland, 1986.